On the Expressibility of Stochastic Switching Circuits

Hongchao Zhou
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA 91125, USA
hzhou@caltech.edu

Jehoshua Bruck
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA 91125, USA
bruck@caltech.edu

***Abstract*— Stochastic switching circuits are relay circuits that consist of stochastic switches (that we call pswitches). We study the expressive power of these circuits; in particular, we address the following basic question: given an arbitrary integer q, and a pswitch set $\{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$, can we realize any rational probability with denominator q^n (for arbitrary n) by a simple series-parallel stochastic switching circuit? In this paper, we generalized previous results and prove that when q is a multiple of 2 or 3 the answer is positive. We also show that when q is a prime number the answer is negative. In addition, we prove that any desired probability can be approximated well by a linear in n size circuit, with error less than q^{-n}.**

I. Introduction

Claude Shannon, in his Master's thesis [1], provided the foundation of modern digital circuit design by demonstrating that Boolean algebra can be used to synthesize and simplify switching relay circuits. By replacing deterministic switches with probabilistic switches (pswitches), a new concept called stochastic switching circuit was proposed in [2]. The study of stochastic switching circuits may enhance our understanding of natural systems and help incorporate randomness in engineering system design [3].

A stochastic switching circuit with two terminals can be constructed by composing pswitches, where each pswitch is closed with some probability. The set of possible pswitch closure probabilities from which a circuit is constructed will be referred to as the pswitch set S. We use $P(C)$ to denote the probability that the two terminals of a circuit C are connected, called as the probability of C. Some probability x can be realized iff there exists a circuit C such that $x = P(C)$. Similarly to resistor circuits [4], connecting a single terminal of a switching circuit C_1 (with probability p_1) to one terminal of C_2 (with probability p_2) places them in series, such that the probability of the resulting circuit is $p_1 \cdot p_2$. Connecting both terminals of two switching circuits C_1 and C_2 places them in parallel, such that the probability of the resulting circuit is $1-(1-p_1)(1-p_2) = p_1+p_2-p_1p_2$. In this paper, we focus on simple series-parallel (ssp) switching circuits, where an ssp circuit is either: (1) a single pswitch, or (2) an ssp circuit with an additional pswitch added in series or parallel. In [5], it is shown that ssp switching circuit is robust against the noise of each pswitch. This property is important in understanding of natural systems and the design of engineering systems because a local error in a system is not be amplified.

One of the interesting questions in stochastic switching circuit is: Given a pswitch set S, what probabilities can be realized and how many pswitches are sufficient? In this paper, we consider the case that the pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$. Wilhelm and Bruck [2] proved that if $q = 2$ or $q = 3$, all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized by an ssp circuit with at most n pswitches, which is optimal. They also showed that if $q = 4$, all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized with at most $2n-1$ pswitches. In this paper, we generalize these results as follows:

- If q is an even number, all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized by an ssp circuit with at most $\lceil \log_2 q \rceil (n-1)+1$ pswitches.
- If q is a multiple of 3, all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized by an ssp circuit with at most $\lceil \log_3 q \rceil (n-1)+1$ pswitches.

However, given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$ with q not a multiple of 2 or 3, then not all $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized, even with an unlimited number of pswitches. In this paper, we will show that if q is a prime number greater than 3, there exists at least one rational $\frac{a}{q^n}$ with $0 < a < q^n$ that cannot be realized with an sp (series-parallel) circuit [1], that is either a single pswitch or an sp circuit connected in series or parallel with another sp circuit.

In the case that q is a prime number greater than 3, or in the case that the desired probability is not rational (such as $\frac{\sqrt{2}}{2}$), it is possible that the desired probability cannot be realized. However, can we use an ssp circuit to get a good approximation of the desired probability? The answer is yes and is given by:

- If q is an integer greater than one, for all desired probability p $(0 < p < 1)$, there exists an ssp circuit C with at most $2n-1$ pswitches such that $|P(C)-p| \leq \frac{1}{2q^n}$.

The remainder of this paper is organized as follows. In Section II, we discuss the case that q is a multiple of 2 or 3. Section III proves that if q is a prime number larger than 3, there exists a rational $\frac{a}{q^n}$ that cannot be realized with series-parallel circuits. However, an approximate rational with small enough error can be realized by an ssp circuit with a bounded

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

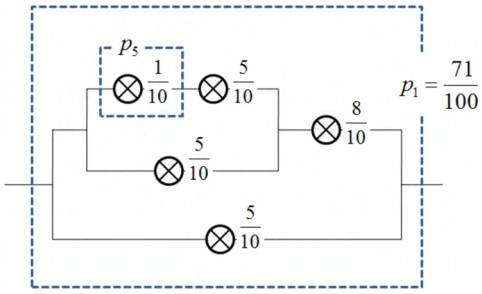


Fig. 1. This circuit realizes $\frac{71}{100}$ for a given pswitch set $S = \{\frac{1}{10}, \frac{2}{10}, ..., \frac{9}{10}\}$, using Algorithm 1.

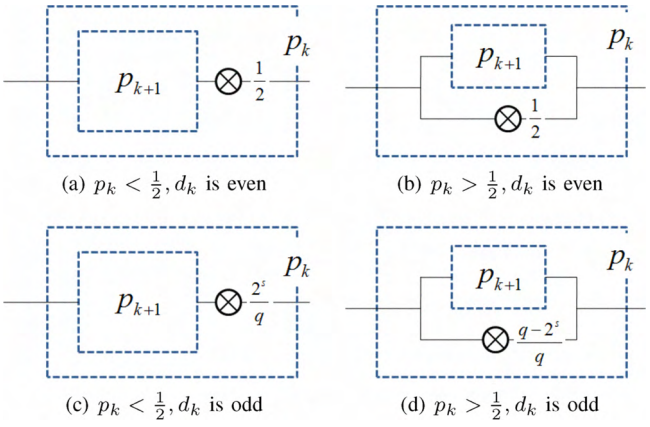


Fig. 2. The way to find p_{k+1} from p_k when q is an even number, where $s = \lfloor \log_2 q \rfloor$.

number of pswitches, as described in Section IV.

II. q IS A MULTIPLE OF 2 OR 3

In this section, we first consider the case that q is an even number for a given pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$. We will show that using the following backward algorithm for even q, all rational $\frac{a}{q^n}$ $(0 < a < q^n)$ can be realized with a bounded number of pswitches.

The basic idea of the backward algorithm is to build the circuit last-pswitch first. If we want to realize a rational p_1, we can find another rational p_2 such that if p_2 can be realized, then p_1 can be realized by adding a single pswitch x to p_2 in series or parallel. So, we can insert the pswitch x as the last pswitch and try to realize p_2 instead of p_1. We continue this process recursively until for some m the rational p_m can be realized with a single pswitch. Then, the circuit realizing p_1 is constructed. The detailed algorithm to construct a circuit C to realize $p_1 = \frac{a}{q^n}$ for an even q is described in Algorithm 1. See Fig. 1 as an example.

Theorem 1. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ...\frac{q-1}{q}\}$ with even q, using Algorithm 1 any rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized by an ssp circuit with at most $\lceil \log_2 q \rceil (n-1)+1$ pswitches.*

Proof: In Algorithm 1, we introduced a parameter $d_k = \frac{q^{w-1}}{gcd(b, q^{w-1})}$ where $\frac{b}{q^w} = p_k$, we can see that d_k has the following properties:

Algorithm 1 Backward algorithm to realize p_1 for an even q

$k = 1$, start with an empty circuit.
while p_k cannot be realized with a single pswitch. **do**
a) Write p_k as $\frac{b}{q^w}$, let $d_k = \frac{q^{w-1}}{gcd(b,q^{w-1})}$*, where $gcd(x, y)$ is the greatest common divisor between x and y.
b) Insert one pswitch to the circuit (see Fig.2)
i) **if** $p_k < \frac{1}{2}$ and d_k is even
Insert one pswitch $\frac{1}{2}$ in series.
Let $p_{k+1} = 2p_k$.
ii) **if** $p_k > \frac{1}{2}$ and d_k is even
Insert one pswitch $\frac{1}{2}$ in parallel.
Let $p_{k+1} = 2p_k - 1$.
iii) **if** $p_k < \frac{1}{2}$ and d_k is odd.
Insert a pswitch $\frac{2^s}{q}$ in series with $s = \lfloor \log_2 q \rfloor$.
Let $p_{k+1} = \frac{q}{2^s} p_k$.
iv) **if** If $p_k > \frac{1}{2}$ and d_k is odd.
Insert a pswitch $\frac{q-2^s}{q}$ in parallel with $s = \lfloor \log_2 q \rfloor$.
Let $p_{k+1} = \frac{q}{2^s}(p_k - \frac{q-2^s}{q})$.
c) $k = k + 1$
end while
Insert one pswitch p_k to the circuit.
*Note that d_k keeps unchanged if we write p_k as $\frac{bc}{q^w c}$ instead of $\frac{b}{q^w}$.

(1) d_k only depends on p_k, if b and q^w multiple the same number at the same time, d_k keeps unchanged.

(2) If $d_k = 1$, p_k can be realized with only one pswitch, and Algorithm 1 stops.

(3) If d_k is even, we have d_{k+1} is a factor of $\frac{d_k}{2}$.

(4) If d_k is odd, we have d_{k+1} is a factor of $\frac{2^s d_k}{gcd(q, 2^s d_k)}$.

Now we give a proof of property (4) under the case (d) in Fig. 2, we have

$$p_{k+1} = \frac{q}{2^s}(p_k - \frac{q-2^s}{q})$$

where p_k can be written as $\frac{b}{q^w}$, then we have

$$p_{k+1} = \frac{q}{2^s}(\frac{b}{q^w} - \frac{q-2^s}{q}) = \frac{q(\frac{q}{2})^s(b - q^{w-1}(q-2^s)}{q^{w+s}}$$

Now, let $g = gcd(b, q^{w-1})$, according to the definition of d_k, we have $q^{w-1} = g \cdot d_k$ and $b = c \cdot g$ for some c, where $gcd(c, d_k) = 1$.

Then, we can get

$$\begin{aligned} d_{k+1} &= \frac{g d_k q^s}{gcd(q(\frac{q}{2})^s(cg - g d_k(q-2^s)), g d_k q^s)} \\ &= \frac{2^s d_k}{gcd(q(c - d_k(q-2^s)), 2^s d_k)} \\ &= \text{a factor of } \frac{2^s d_k}{gcd(q, 2^s d_k)} \end{aligned}$$

According to the properties (1)-(4) of d_k, we can see that d_k is bounded since $d_1 \le q^{n-1}$ and in each step d_k decreases. Therefore, within a limited number of steps, d_k will get 1.

Now, let's define

$$N = \min\{k | k \in (1, 2, 3...), d_k = 1\}$$

Then N is the number of required pswitches in Algorithm 1, so we only need to prove that $N \leq \lceil \log_2 q \rceil (n-1) + 1$.

Since q is even, we can write $q = 2^c$ or $q = 2^c t$ with odd $t > 1$. At first, we consider the case that $q = 2^c$. At the beginning we have d_1 is a factor of q^{n-1}, according to the property (3), we can get

$$N \leq c(n-1) + 1 = \lceil \log_2 q \rceil (n-1) + 1$$

In order to prove the second case that $q = 2^c t$ with odd $t > 1$, we define M_i as the step number that d_k gets odd for the ith times, i.e.

$$M_i = \text{ith smallest element in } \{k | k \in (1, 2, 3...), d_k \text{ is odd}\}$$

According to properties (3)(4) and d_1 is a factor of q^{n-1} at the beginning, we can get d_{M_i} is a factor of q^{n-i}, therefore, there exits a minimal k with $k \leq n$ such that $d_{M_k} = 1$. Then, we can have $N = M_k$.

According to properties (3)(4), we also can get that

$$M_1 \leq c(n-1) + 1$$

$$M_{i+1} - M_i \leq s - c$$

Therefore

$$N \leq \sum_{i=1}^{n-1} (M_{i+1} - M_i) + M_1 \leq s(n-1) + 1$$

$$= \lceil \log_2 q \rceil (n-1) + 1$$

□

Using similar methods, we can prove the following theorems about the upper boundary of optimal circuit size when q is a multiple of 3 or 6.

Theorem 2. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ...\frac{q-1}{q}\}$, if q is odd and is a multiple of 3, then any rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized by an ssp circuit with at most $\lceil \log_3 q \rceil (n-1) + 1$ pswitches.*

Theorem 3. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ...\frac{q-1}{q}\}$, if q is multiple of 6, all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized by an ssp circuit with at most N pswitches, where*

$$N \leq \begin{cases} (2s)(n-1)+1 & (\text{if } 6^s = q) \\ (2s+1)(n-1)+1 & (\text{if } \frac{q}{2} \leq 6^s < q) \\ (2s+2)(n-1)+1 & (\text{if } \frac{q}{3} \leq 6^s < \frac{q}{2}) \\ (2s+3)(n-1)+1 & (\text{if } \frac{q}{6} < 6^s \leq \frac{q}{3}) \end{cases}$$

During the process to construct a circuit in Algorithm 1, in each step the parameter d_k decreases. However, this algorithm is not efficient to realize desired rational since it may use many more pswitches than the optimal size, especially for the case that q is large. In order to overcome this weakness, we propose a greedy backward algorithm (GBA) to realize the desired rational, as described in Algorithm 2. The idea of this algorithm is as the same as Algorithm 1: in each step, we try to insert a pswitch such that $d_{k+1} < d_k$. However, we may have many choices to insert a pswitch in series or in parallel. So among these choices, we select the "best" one such that in each step d_k is minimized and p_k can be written as a fraction with denominator q^w for some w, that is why we call it greedy algorithm. Surprisingly, when q is a multiple of 2 or 3, GBA can realize most of desired probabilities with almost optimal size. Here, we say that a desired probability is realized with optimal size if it cannot be realized with less pswitches. In Fig. 3, for each value $q \in [2, 3, 4, 6, 8, 9, 10]$, we enumerate all rationals with the same optimal size n, then we use GBA to realize these rationals and account the average number of used pswitches. It is shown that GBA can work well to realize

Algorithm 2 Greedy Backward Algorithm to realize p_1

$k = 1$, start with an empty circuit.

while p_k cannot be realized with a single pswitch. **do**

a) Let S denote the set of the ways to insert a pswitch.

$$S = \{(\frac{1}{q}, series), (\frac{1}{q}, parallel), ...\}$$

b) Given p_k and $x \in S$, let $p(p_k, k)$ calculate p_{k+1} corresponding to x. Then, $d(p(p_k, k))$ calculates the corresponding d_{k+1} of x, where

$$d(\frac{b}{q^w}) = \frac{q^{w-1}}{gcd(b, q^{w-1})}$$

c) Let O denote the optimal option to minimize d_{k+1}:

$O = \arg\min_{x \in S} \{d(p(p_k, x)) | p(p_k, x)$ can be written as $\frac{b}{q^w}\}$

Then $p_{k+1} = p(p_k, O)$ and $d_{k+1} = d(p(p_k, O))$.

d) IF $d_{k+1} \geq d(p_k)$

p_1 cannot be realized using GBA. Return.

ELSE

Insert a pswitch according to O.

e) $k = k + 1$

end while

Insert one pswitch p_k to the circuit.

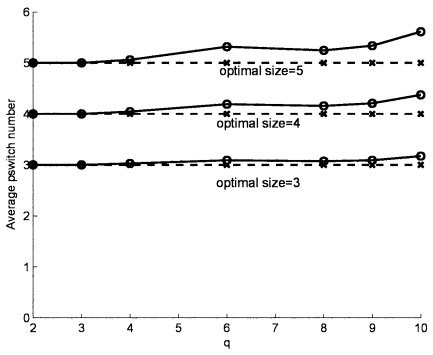


Fig. 3. For each q, the average number of pswtiches used in GBA to realize all the rationals with the same optimal size 3 or 4 or 5.

most of desired probabilities. And, when q is a multiple of 2 or 3, we have the following theorem, but we cannot give a boundary tighter than that in Theorems 1-3.

Theorem 4. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ...\frac{q-1}{q}\}$, if q is a multiple of 2 or 3, then GBA realizes any rational $\frac{a}{q^n}$ such that $0 < a < q^n$ by an ssp circuit.*

III. q IS A PRIME NUMBER GREATER THAN 3

In the above section, we proved that if q is a multiple of 2 or 3, all rational $\frac{a}{q^n}$ can be realized with a bounded number of pswitches. Is this true if q is an arbitrary number greater than 2?

Theorem 5. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$, if a rational $\frac{a}{q^n}$ with q a prime number, cannot be realized by an sp circuit with n pswitches, then it cannot be realized with any number of pswitches using an sp (series-parallel) circuit.*

Proof: Assume that there exits a rational $\frac{a}{q^n}$ cannot be realized by an sp circuit with n pswitch but can be realized with at least $l(l > n)$ pswitches, where l is optimal (minimal) for all fractions with denominator q^k. Now, we want to prove that there exists another rational such that l is not the minimal one.

According to the definition of sp circuits, we know that $\frac{a}{q^n}$ can be realized by connecting two sp circuits C_1 and C_2 in series or in parallel. Assume the first circuit C_1 consists of l_1 pswitches and is closed with probability $\frac{b_1}{q^{l_1}}$, and the second circuit C_2 consists of l_2 pswitches and is closed with probability $\frac{b_2}{q^{l_2}}$, where $l_1 + l_2 = l$.

If C_1 and C_2 are connected in series, we can get

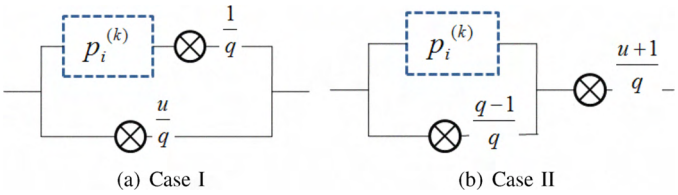
$$\frac{b_1}{q^{l_1}}\frac{b_2}{q^{l_2}} = \frac{a}{q^n}$$

Therefore $b_1 b_2 = aq^{l-n}$, $b_1 b_2$ is a multiple of q. Since q is a prime number, either b_1 or b_2 is a multiple of q. Without loss of generality, we assume b_1 is a multiple of q, therefore b_1 can be written as cq. Let's consider the rational $\frac{c}{q^{l_1-1}}$, it can be realized with C_1 consisting l_1 pswitches. Assume it can also be realized with another sp circuit C_3 with $l_1 - 1$ pswitches, then by connecting C_3 and C_2 in series, we can realize $\frac{a}{q^n}$ with $l_1 - 1 + l_2 = l - 1$ pswitches, which conflicts with our assumption that $\frac{a}{q^n}$ cannot be realized with less than l pswitches. Then we have that $\frac{c}{q^{l_1-1}}$ can be not realized with $l_1 - 1$ pswitches, but it can be realized with l_1 pswiches. However, $l_1 < l$, which also conflicts with the assumption that l is optimal.

If C_1 and C_2 are connected in parallel, we can get

$$\frac{b_1}{q^{l_1}} + \frac{b_2}{q^{l_2}} - \frac{b_1}{q^{l_1}}\frac{b_2}{q^{l_2}} = \frac{a}{q^n}$$

Therefore $b_1 b_2 = b_1 q^{l_2} + b_2 q^{l_1} - aq^{l-n}$. Similar as above, we can conclude that either b_1 or b_2 is a multiple of q. Finally, this will lead to either (1) $\frac{a}{q^l}$ can be realized with less than l pswitches or (2) l is not optimal. We reach a contradiction, hence, we have the conclusion in the theorem. □



(a) Case I (b) Case II

Fig. 4. Operate the rationals in F_k in two ways, where $u = 0, 1, ..., q-1$

Theorem 6. *For a prime number $q > 3$, there exists an integer a (where $0 < a < q^n$) such that $\frac{a}{q^n}$ cannot be realized by an sp circuit for $n \geq 2$.*

Proof: In [2], the following result is given: No pswitch set containing all $\frac{a}{q}$, $0 < a < q$, for any $q > 3$, can realize all $P_r(C) = \frac{b}{q^2}$ $(0 < b < q^2)$ with at most 2 pswitches. The conclusion follows from this result and Theorem 5. □

IV. CIRCUITS FOR APPROXIMATING PROBABILITIES

If a desired probability can never be realized using the pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ...\frac{q-1}{q}\}$, for example the desired probability is not a rational, can we construct a circuit to realize an approximate probability? And how many pswitches are needed to achieve a required accuracy?

Theorem 7. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}...\frac{q-1}{q}\}$, for any desired probability p_d, there exists a rational probability p_a such that $|p_a - p_d| \leq \frac{1}{2q^n}$ and p_a can be realized by an ssp circuit with at most $2n-1$ pswitches.*

Proof: Assume F_n is the set of rationals that can be realized with at most $2n-1$ pswitches. It can be written as $F_n = \{p_1^{(n)}, p_2^{(n)}, p_3^{(n)}...p_{m_n}^{(n)}\}$ where m_n is the number of rationals that can be realized, and $p_1^{(n)} = 0 < p_2^{(n)} < ... < p_{m_n}^{(n)} = 1$. We can prove this theorem by induction. For $n = 1$, the statement is true. Assume for any probability $p_d^{(k)}$, there exists a rational $p_a^{(k)} \in F_k$ such that $|p_a^{(k)} - p_d^{(k)}| \leq \frac{1}{2q^k}$. Then, we want to prove that for any probability $p_d^{(k+1)}$, there exists a rational $p_a^{(k+1)} \in F_{k+1}$ such that $|p_a^{(k+1)} - p_d^{(k+1)}| \leq \frac{1}{2q^{k+1}}$.

(1) If $p_d^{(k+1)} \in [\frac{u}{q}, \frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}]$ for some $u \in \{0, 1, ..., q-1\}$. Let

$$p_d^{(k)} = \frac{p_d^{(k+1)} - \frac{u}{q}}{\frac{1}{q} - \frac{u}{q^2}}$$

Since $\frac{u}{q} \leq p_d^{(k+1)} \leq \frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}$, we have $0 \leq p_d^{(k)} \leq 1$. For $p_d^{(k)}$, according to our assumption, there exists a rational $p_a^{(k)} \in F_k$ such that $|p_a^{(k)} - p_d^{(k)}| \leq \frac{1}{2q^k}$.

Now, we can get $p_a^{(k+1)}$ from $p_a^{(k)}$ by adding a $\frac{1}{q}$ pswitch in series and a $\frac{u}{q}$ pswitch in parallel (see Fig. 4(a)). Note if $u = 0$, then we do not add the pswitch. Since $p_a^{(k)}$ can be realized with at most $2k-1$ pswitches, $p_a^{(k+1)}$ can be realized with at most $2(k+1)-1$ pswitches. Therefore, $p_a^{(k+1)} \in F_{k+1}$. $p_a^{(k)}$ and $p_a^{(k+1)}$ have the following relation:

$$p_a^{(k)} = \frac{p_a^{(k+1)} - \frac{u}{q}}{\frac{1}{q} - \frac{u}{q^2}}$$

and

$$|p_a^{(k)} - p_d^{(k)}| = |\frac{p_a^{(k+1)} - \frac{u}{q}}{\frac{1}{q} - \frac{u}{q^2}} - \frac{p_d^{(k+1)} - \frac{u}{q}}{\frac{1}{q} - \frac{u}{q^2}}| \leq \frac{1}{2q^k}$$

which can be simplified as

$$|p_a^{(k+1)} - p_d^{(k+1)}| \leq \frac{1}{2q^k}(\frac{1}{q} - \frac{u}{q^2}) \leq \frac{1}{2q^{k+1}}$$

(2) If $p_d^{(k+1)} \in [\frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}, \frac{u+1}{q}]$ for some $u \in \{0, 1, ..., q-1\}$. Let

$$p_d^{(k)} = (p_d^{(k+1)} \frac{q}{u+1} - \frac{q-1}{q})q$$

Since $\frac{u}{q} + \frac{1}{q} - \frac{u}{q^2} \leq p_d^{(k+1)} \leq \frac{u+1}{q}$, we have $\frac{1}{u+1} \leq p_d^{(k)} \leq 1$. For $p_d^{(k)}$, according to our assumption, there exists a rational $p_a^{(k)} \in F_k$ such that $|p_a^{(k)} - p_d^{(k)}| \leq \frac{1}{2q^k}$.

Now, we can get $p_a^{(k+1)}$ from $p_a^{(k)}$ by adding an $\frac{q-1}{q}$ pswitch in parallel and a $\frac{u+1}{q}$ pswitch in series (see Fig. 4(b)). Since $p_a^{(k)}$ can be realized with at most $2k-1$ pswitches, $p_a^{(k+1)}$ can be realized with at most $2(k+1)-1$ pswitches. Therefore, $p_a^{(k+1)} \in F_{k+1}$. $p_a^{(k)}$ and $p_a^{(k+1)}$ have the following relation:

$$p_a^{(k)} = (p_a^{(k+1)} \frac{q}{u+1} - \frac{q-1}{q})q$$

and

$$|p_a^{(k)} - p_d^{(k)}| = |p_a^{(k+1)} \frac{q^2}{u+1} - p_d^{(k+1)} \frac{q^2}{u+1}| \leq \frac{1}{2q^k}$$

which can be simplified as

$$|p_a^{(k+1)} - p_d^{(k+1)}| \leq \frac{1}{2q^k} \frac{u+1}{q^2} \leq \frac{1}{2q^{k+1}}$$

For all $p_d^{(k+1)} (0 \leq p_d^{k+1} \leq 1)$, either $p_d^{(k+1)} \in [\frac{u}{q}, \frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}]$ or $p_d^{(k+1)} \in [\frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}, \frac{u+1}{q}]$ for some $u \in \{0, 1, ..., q-1\}$. So we can conclude that if the statement is true for $n = k$, then it is also true for $n = k+1$. Therefore, we can conclude that for any desired probability $p_d (0 \leq p_d \leq 1)$, there exists a rational $p_d \in F_n$ such that $|p_a - p_d| \leq \frac{1}{2q^n}$ □

Based on this proof, we can use Algorithm 3 to construct a circuit to get a good approximation of the desired probability with error smaller than ϵ. We can conclude that there are at most $2\lceil \log_q \frac{1}{2\epsilon} \rceil - 1$ pswitches in the circuit.

For the special case of $q = 2$ or $q = 3$, we can also obtain the following theorem:

Theorem 8. *Given a pswitch set $S = \{0, \frac{1}{q}, \frac{2}{q} ... \frac{q-1}{q}\}$ with $q = 2$ or 3, for any desired probability p_d $(0 \leq p_d \leq 1)$, there exists a rational p_a $(0 \leq p_a \leq 1)$ such that $|p_a - p_d| \leq \frac{1}{2q^n}$ and p_a can be realized by an ssp circuit with at most n pswitches.*

Proof: This theorem is a corollary of the following theorem [2]: Given a pswitch set $S = \{0, \frac{1}{q}, \frac{2}{q} ... \frac{q-1}{q}\}$ with $q = 2$ or $q = 3$, all rational $\frac{a}{q^n} (0 < a < q^n)$ can be realized with at most n pswitches. □

According to this theorem, given a pswitch set $S = \{\frac{1}{2}\}$ or $S = \{\frac{1}{3}, \frac{2}{3}\}$, if we want to realize p_d with error smaller than ϵ, we can construct a circuit closed with probability $p_a = \frac{a}{q^n}$ with $n = \lceil \log_q \frac{1}{2\epsilon} \rceil$ and $|p_d - p_a| < \epsilon$. Using the algorithms in [2], p_a can be realized with at most $\lceil \log_q \frac{1}{2\epsilon} \rceil$ pswitches.

Algorithm 3 Backward algorithm to realize p_1 with error$< \epsilon_1$.

$k = 1$, start with an empty circuit

while $|\frac{i}{q} - p_k| > \epsilon_k$, $\forall i \in \{0, 1, 2...q\}$ **do**

a) **if** $p_k \in [\frac{u}{q}, \frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}]$ for some $u \in \{0, 1, ..., q-1\}$ Insert a $\frac{u}{q}$ pswitch in parallel, and then insert a $\frac{1}{q}$ pswitch in series. (see Fig. 4(a)) Let

$$p_{k+1} = \frac{p_k - \frac{u}{q}}{\frac{1}{q} - \frac{u}{q^2}}, \epsilon_{k+1} = \frac{q^2 \epsilon_k}{q-u}$$

b) **if** $p_k \in [\frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}, \frac{u+1}{q}]$ for some $u \in \{0, 1...q-1\}$ Insert a $\frac{u+1}{q}$ pswitch in series, and then insert a $\frac{q-1}{q}$ pswitch in parallel.(see Fig. 4(b)) Let

$$p_{k+1} = (p_k \frac{q}{u+1} - \frac{q-1}{q})q, \epsilon_{k+1} = \frac{q^2 \epsilon_k}{u+1}$$

c) $k = k + 1$

end while

Let $u = \arg\min_i |\frac{i}{q} - p_k|$ and insert an $\frac{u}{q}$ pswitch to replace p_k.

V. Conclusion

In this paper, we generalized the results in [2] and proved that when q is a multiple of 2 or 3, all rational fractions $\frac{a}{q^n}$ can be realized with pswitches, each closed with a probability in $\{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$. However, this property does not hold when q is a prime number greater than 3. Finally, we proved that any desired probability can be approximated well by a linear size ssp circuit.

There are a number of open problems, for example, how to construct an optimal stochastic switching circuit with an arbitrary pswitch set? If q is neither a prime number nor a multiple of 2 or 3 (like $q = 25$), can we realize all rationals $\frac{a}{q^n}$ using a simple series-parallel circuit?

Acknowledgment

This work was supported in part by the NSF Expeditions in Computing Program under grant CCF-0832824. The authors would like to thank Dan Wilhelm for discussions and assistance.

References

[1] C.E. Shannon. A symbolic analysis of relay and switching circuits. Trans. AIEE, 57:713-723, 1938.

[2] D. Wihelm, J. Bruck. Stochastic switching circuit synthesis. IEEE International Symposium on Information Theory(ISIT), 2008. 1388-1392.

[3] B. Fett, J. Bruck, and M.D. Riedel. Synthesizing stochasticity in biochemical systems. In Proceedings of the 44th Annual Conference on Design Automation(DAC), 2007. 640-645.

[4] P.A. MacMahon. The combinations of resistances. The Electrician, 28:601C602, 1892. (Reprinted in: Discr. Appl. Math., 54:225-228, 1994.).

[5] P. Loh, H. Zhou and J. Bruck. The Robustness of Stochastic Switching Networks. IEEE International Symposium on Information Theory(ISIT), 2009.